UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
JOSEPH FELDMAN and
VANDERBILT HOME PRODUCTS, LLC,

Plaintiffs,

-against-

COMP TRADING, LLC; MOSES TAWIL; JONATHAN TAWIL; MICHAEL SASSON; HARRY HIDARY; and EDDIE SITT,

Defendants.
----------X

MEMORANDUM AND ORDER
19-CV-4452 (RPK) (RLM)

RACHEL P. KOVNER, United States District Judge:

Plaintiffs Joseph Feldman and Vanderbilt Home Product, LLC, bring this action against Comp Trading, LLC and several of Comp Trading's members. Plaintiffs allege that defendants violated the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, and the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, by accessing Feldman's email account without his authorization. Defendants have moved to dismiss the complaint for failure to state a claim. For the reasons set out below, the motion to dismiss is denied.

BACKGROUND

Plaintiffs are Joseph Feldman, an individual and a former member of the New York limited liability company Comp Trading, LLC ("Comp Trading"), and Vanderbilt Home Products, LLC ("Vanderbilt"), a New Jersey limited liability company whose principal place of business is in New York. Compl. ¶¶ 3, 4 (Dkt. #1). Plaintiffs filed the initial complaint in this case in August 2019, alleging violations of the SCA and CFAA. *Id.* ¶¶ 2, 11. Plaintiffs named as defendants Comp Trading; Moses Tawil, president and chief executive officer of Comp Trading; Eddie Sitt,

chief technology officer of Comp Trading; and Jonathan Tawil, Michael Sasson, and Harry Hidary, members of Comp Trading. *Id.* ¶¶ 5-10.

Defendants filed an answer to the complaint, and soon afterward, filed a letter requesting a pre-motion conference regarding an anticipated motion for judgment on the pleadings. *See generally* Answer (Dkt. #9); Letter Motion for Pre-Motion Conference ("Defs.' PMC Letter") (Dkt. #23). Defendants primarily argued that plaintiffs failed to state a claim under the CFAA because they had not alleged that they suffered a "loss" within the meaning of that statute. *See* Defs.' PMC Letter at 2. The Court held a pre-motion conference, set a deadline for plaintiffs to file an amended complaint, and set a briefing schedule for defendants' anticipated motion to dismiss the amended complaint. *See* Minute Entry and Order dated Mar. 31, 2020.

Plaintiffs then filed the now-operative amended complaint. *See* Am. Compl. (Dkt. #33). The amended complaint alleges that in December 2017, while Feldman still held a membership interest in Comp Trading, Vanderbilt registered an email address for Feldman ("the Feldman account") through Microsoft's cloud-based email hosting service, Microsoft 365. *Id.* ¶¶ 13, 20. Feldman was the sole user of the account and never gave anyone else the authorization or the means to access the account. *Id.* ¶¶ 18, 19. According to the complaint, Feldman used the account to maintain private email communications and documents. *Id.* ¶ 14. In June 2018, Feldman divested himself of his membership interest in Comp Trading. *Id.* ¶ 20.

The amended complaint alleges that in April 2019, defendants, acting in concert with one another and on behalf of Comp Trading, began to access the Feldman account "to access, intercept and steal confidential, proprietary and trade secret business information, private and confidential personal information, and attorney-client privileged communications." *Id.* ¶¶ 21, 36. Plaintiffs

allege that defendants accessed the Feldman account at least 117 times between April 29, 2019 and June 19, 2019, when Feldman found out and took measures to prevent it from continuing. *Id.* ¶¶ 22-24, 26. Plaintiffs add that defendants "downloaded, viewed and disseminated" information taken from the Feldman account "amongst themselves and to unauthorized third parties." *Id.* ¶ 25; *see id.* ¶¶ 22-23, 29-30. The documents and information "were electronically stored on the Microsoft 365 cloud server, which is owned and controlled by Microsoft, an electronic service provider." *Id.* ¶ 32; *see id.* ¶ 38.

Plaintiffs allege that they suffered losses of over $5,000 in the last year "in connection with identifying evidence of a breach" to the Feldman account, "assessing any damage such breach may have caused," "determining whether any remedial measures were necessary, and implementing such remedial measures." *Id.* ¶ 40. In particular, plaintiffs allege that they paid at least $2,000 in fees to "IT specialists" to investigate, remedy, and secure the Feldman account and other potentially at-risk email accounts; paid at least $2,300 in fees to attorneys "for investigative costs"; and incurred at least $4,000 "in lost employee time diverted to the investigation and remediation of the breach" of the Feldman account. *Id.* ¶ 41.

Plaintiffs allege that defendants' access of the Feldman account violated the SCA and CFAA. *Id.* ¶¶ 27-43. As relief, plaintiffs seek compensatory, statutory, and punitive damages, as well as costs, interest, and attorney's fees. *Id.* ¶¶ 34, 40-43; *see id.* at 8. Plaintiffs also seek various injunctive relief. *Id.* at 8.

Defendants have moved to dismiss the complaint for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). *See generally* Mem. of L. in Supp. of Mot. to Dismiss ("Defs.' Br.") (Dkt. #36). As explained below, defendants' motion to dismiss the amended

complaint is denied, because plaintiffs have adequately pleaded claims under the SCA and the CFAA.

DISCUSSION

Federal Rule of Civil Procedure 12(b)(6) directs a court to dismiss a complaint that fails "to state a claim upon which relief can be granted." To avoid dismissal on this basis, a complaint must "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The facial "plausibility standard is not akin to a 'probability requirement.'" *Ibid.* (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556, 570 (2007)). But it requires a plaintiff to allege sufficient facts to enable the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ibid.* "A well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof [of the facts alleged] is improbable, and that a recovery is very remote and unlikely." *Twombly*, 550 U.S. at 556 (quotations omitted). In evaluating a motion to dismiss under Rule 12(b)(6), the court must accept all facts alleged in the complaint as true. *Iqbal*, 556 U.S. at 678. The court, however, is not obligated to adopt "[t]hreadbare recitals of the elements of a cause of action" that are "supported by mere conclusory statements." *Ibid.*

I. Group Pleading

Defendants first argue that the amended complaint should be dismissed because it does not satisfy the minimum pleading requirements of Federal Rule of Civil Procedure 8 due to impermissible group pleading. *See* Defs.' Br. at 5-7. Specifically, defendants argue that the complaint uses impermissible group pleading because it does not state "which of the six separate, independent defendants" accessed the Feldman account. *Id.* at 5. Plaintiffs contend that the amended complaint satisfies Rule 8 and further argue that defendants waived this argument by

failing to raise it earlier in the litigation. *See* Mem. of L. in Opp'n to Mot. to Dismiss at 16 ("Pls.' Br.") (Dkt. #41). As explained below, defendants have not waived their group-pleading argument, but the argument fails on the merits.

A. Waiver

As an initial matter, defendants did not waive their group-pleading argument by failing to raise it earlier. As plaintiffs observe, defendants did not raise a group-pleading argument in their answer to the original complaint. But the amended complaint "supersede[d] the original, and render[ed] it of no legal effect." *Shields v. Citytrust Bancorp, Inc.*, 25 F.3d 1124, 1128 (2d Cir. 1994) (quoting *Int'l Controls Corp. v. Vesco*, 556 F.2d 665, 668 (2d Cir. 1977)). When an amended complaint has been filed, the only defenses that are waived because they were not contained in an earlier answer are "those that involve the core issue of a party's willingness to submit a dispute to judicial resolution, such as objections to lack of personal jurisdiction, improper venue, insufficiency of process and insufficiency of service." *Ibid.* (quotations omitted). Plaintiffs' argument that the complaint fails to state a claim on which relief can be granted is not one of those defenses. *See* Fed. R. Civ. P. 12(h)(2) (providing that "[f]ailure to state a claim upon which relief can be granted . . . may be raised . . . in any pleading allowed or ordered under Rule 7(a)," including "an answer to a complaint"); 5C Charles Alan Wright & Arthur A. Miller, Federal Practice & Procedure § 1392 (3d ed. 2020) (explaining that defenses set out in Rule 12(h)(2) are not waived merely because they were not raised in the first responsive pleading); *see also In re Parmalat Sec. Litig.*, 421 F. Supp. 2d 703, 713 (S.D.N.Y. 2006).

Nor did defendants waive their group-pleading argument by failing to raise it in their request for a pre-motion conference. While a defendant ordinarily may not file a second motion

to dismiss to "advance arguments that could have been made in [a] first motion to dismiss," *Sears Petroleum & Transp. Corp. v. Ice Ban Am., Inc.*, 217 F.R.D. 305, 307 (N.D.N.Y. 2003), a pre-motion conference letter does not qualify as a prior "motion to dismiss." *See Schweitzer ex rel. Schweitzer v. Crofton*, No. 8-CV-135, 2010 WL 3516161, at *7 (E.D.N.Y. Sept. 1, 2010) (explaining that "a pre-motion conference letter" does not constitute "a 'motion' under Rule 12 such that a failure to raise a defense in such a letter results in a waiver of that defense"), *aff'd sub nom. Schweitzer v. Crofton*, 560 F. App'x 6 (2d Cir. 2014); *see also JP Morgan Chase Bank, N.A. v. Law Office of Robert Jay Gumenick, P.C.*, No. 8-CV-2154, 2011 WL 1796298, at *3 (S.D.N.Y. Apr. 22, 2011).

B. Plaintiffs' Collective Allegations

Defendants' group-pleading argument nevertheless fails on the merits. Courts in this circuit have evaluated CFAA claims under Federal Rule of Civil Procedure 8(a), which requires that a complaint "contain . . . a short and plain statement of the claim showing that the pleader is entitled to relief." *See Dedalus Found. v. Banach*, No. 9-CV-2842, 2009 WL 3398595, at *4 (S.D.N.Y. Oct. 16, 2009) ("A plaintiff asserting a CFAA claim, must only allege the required elements pursuant to Rule 8(a)(2)'s notice pleading standard, not Rule 9(b)'s heightened pleading standard."); *see also JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 526 (S.D.N.Y. 2013); *DCR Mktg. Inc. v. Pereira*, No. 19-CV-3249, 2020 WL 91495, at *2 (S.D.N.Y. Jan. 8, 2020). Some courts have applied the heightened pleading standards for fraud claims in Federal Rule of Civil Procedure 9 to a subset of CFAA claims: those arising under 18 U.S.C. § 1030(a)(4), which prohibits the unauthorized access of a computer "with intent to defraud." *Compare Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1072 (N.D. Cal. 2018) (applying Rule 9 to a

claim under Section 1030(a)(4)), *with NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 834 (N.D. Cal. 2014) (holding that Rule 9 did not apply to all Section 1030(a)(4) claims), *and Sprint Nextel Corp. v. Simple Cell, Inc.*, No. 13-CV-617, 2013 WL 3776933, at *6 (D. Md. July 17, 2013) ("The balance of authority . . . appears to support the view that Rule 9(b) does not apply to § 1030(a)(4)."). But the amended complaint makes no suggestion that defendants violated Section 1030(a)(4) or that plaintiffs' claims otherwise sound in fraud. *See* Am. Compl. ¶¶ 35-43. The complaint is therefore evaluated under Rule 8, not Rule 9.

Rule 8 imposes a "lenient standard" for pleading. *Wynder v. McMahon*, 360 F.3d 73, 80 (2d Cir. 2004). A complaint "need only 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.'" *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (quoting *Twombly*, 50 U.S. at 555). Applying this principle, the Second Circuit has affirmed the dismissal of a complaint that alleged "a host of constitutional and state law claims . . . by 'the defendants,' and failed to identify any factual basis for the legal claims made." *Atuahene v. City of Hartford*, 10 F. App'x 33, 34 (2d Cir. May 31, 2001). The court of appeals stated that the complaint impermissibly "lump[ed] all the defendants together in each claim and provid[ed] no factual basis to distinguish their conduct." *Ibid.* But the Second Circuit has also held that "Rule 8 does not necessarily require . . . that the complaint separate out claims against individual defendants." *Wynder*, 360 F.3d at 80. That is, "[n]othing in Rule 8 prohibits collectively referring to multiple defendants where the complaint alerts defendants that identical claims are asserted against each defendant." *Manchanda v. Navient Student Loans*, No. 19-CV-5121, 2020 WL 5802238, at *2 (S.D.N.Y. Sept. 29, 2020); *see Vaad Hakashrus Crown Heights Inc. v. Braun*, No. 15-CV-5857, 2017 WL 10180422, at *5 (E.D.N.Y. Jan. 12, 2017) (same); *Vantone Grp. Liab. Co. v. Yangpu*

NGT Indus. Co., No. 13-CV-7639, 2015 WL 4040882, at *3 (S.D.N.Y. July 2, 2015) (same). The question is ultimately whether the complaint gives each party "notice of the substance of the claims against him." *OneWest Bank N.A. v. Lehman Bros. Holding Inc.*, No. 14-CV-8916, 2015 WL 1808947, at *3 (S.D.N.Y. Apr. 20, 2015); *see Canosa v. Ziff*, No. 18-CV-4115, 2019 WL 498865, at *10 (S.D.N.Y. Jan. 28, 2019).

The amended complaint in this case gives the defendants adequate notice. It alleges that each of the defendants accessed the Feldman account, in violation of the CFAA, and that each of the defendants "downloaded, viewed, and disseminated" information from that account. Am. Compl. ¶¶ 5-10, 21, 23, 29, 30, 36. It thus puts the defendants on notice of the substance of the claims against them and the grounds on which those claims rest. The motion to dismiss for impermissible group pleading is therefore denied.

II. Stored Communications Act Claim

Defendants next argue that plaintiffs have failed to state a claim under the SCA. As relevant here, the SCA creates a private right of action against a party who "intentionally exceeds an authorization to access" a facility through which an electronic communication service is provided, "and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a)(2) (describing the offense); *see id.* § 2707(a) (providing for civil enforcement). The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17). To allege a violation of these provisions, plaintiffs claim that

defendants hacked into an account on Microsoft's "cloud-based email hosting service, Microsoft 365," and "illegally accessed" documents and information that "were electronically stored on the Microsoft 365 cloud server, which is owned and controlled by Microsoft, an electronic communication service provider." Am. Compl. ¶¶ 13, 21, 23, 32. Defendants argue that the amended complaint falls short because it does not allege that the email messages accessed by defendants were unopened. In defendants' view, this omission is fatal because only unopened messages are in "electronic storage" for purposes of the SCA. *See* Defs.' Br. at 7-8.

Defendants' motion to dismiss on these grounds is denied. There is robust debate over whether only unopened emails are in "electronic storage" for the purposes of the SCA. *Compare Hately v. Watts*, 917 F.3d 770, 786 (4th Cir. 2019) (holding that "previously opened and delivered emails fall within" Section 2510(17)(B)); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) (similar), *with United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (holding that previously opened emails stored on a web-based email system are not "in electronic storage"); *see also Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 227 n.4 (2d Cir. 2016) (Lynch, J., concurring) (noting that the Second Circuit "ha[s] not addressed the issue" of whether "once the user of an entirely web-based email service" opens an email, "that email is no longer 'in electronic storage'"), *vacated on other grounds sub nom. United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018). But courts have consistently rejected the argument that a plaintiff must make allegations that are more specific than those in the amended complaint to survive a motion to dismiss. *See Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782, 788-90 (N.D. Ill. 2014); *see Loughnane v. Rogers,* No. 19-CV-86, 2019 WL 4242486, at *3 (N.D. Ill. Sept. 6, 2019); *Kaufman v. Nest Seekers, LLC*, No. 5-CV-6782, 2006 WL

2807177, at *7 (S.D.N.Y. Sept. 26, 2006). Those courts have reasoned that Rule 8(a)'s requirement of a short and plain statement of a plaintiff's claims does not demand detailed allegations on why communications were in "electronic storage." *Jin*, 75 F. Supp. 3d at 788; *Loughnane*, 2019 WL 4242486, at *3. Plaintiffs' allegations that defendants illegally accessed documents "electronically stored" on a cloud-based email hosting service are sufficient under Rule 8(a) to survive a motion to dismiss.

III. Computer Fraud and Abuse Act Claim

Defendants next argue that plaintiffs failed to state a claim under the CFAA because they do not adequately allege damages that are cognizable under that statute. *See* Defs.' Br. at 8-12. As explained below, that argument lacks merit.

A. Statutory Framework

A violation of the CFAA occurs when, among other things, a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer," 18 U.S.C. § 1030(a)(2)(C), or "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or . . . intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss," *id.* § 1030(a)(5). The CFAA's civil enforcement provision allows "[a]ny person who suffers damage or loss" from conduct prohibited by the statute to bring a private action if the plaintiff can satisfy one of five requirements. *See Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 562 (2d Cir. 2006) (quoting 18 U.S.C. § 1030(g)). One such requirement is that a party has suffered "loss" of at least $5,000 "during any 1-year period." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

The CFAA defines the terms "computer," "protected computer," "loss," and "damage." *See* 18 U.S.C. § 1030(e). A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." *Id.* § 1030(e)(1). A "protected computer" means a "computer . . . used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2).

In addition, the CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). And "damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8).

B. Discussion

Plaintiffs have adequately alleged that they "suffered aggregated losses of over $5,000 during the last 1-year period" as a result of defendants' violations of the CFAA. Am. Compl. ¶ 40; *see id.* ¶¶ 41-42. Plaintiffs rely on payments to information technology specialists and attorneys to investigate, remedy, and secure the Feldman account, as well as "lost employee time diverted to the investigation and remediation of the breach." *Id.* ¶¶ 40-41. These expenditures fall within the CFAA's definition of "loss," which includes "any reasonable cost to any victim," including the costs of "responding to an offense," as well as "conducting a damage assessment"

and "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Defendants suggest that these losses are not cognizable because they were not costs to remedy or investigate "damage" to plaintiffs' computers or to Microsoft's servers. Defs.' Br. at 9-11. But the CFAA's definition of costs is not limited to costs flowing directly in this way from "damage"—that is, from "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Instead, the CFAA's definition of "loss" extends to "any reasonable cost to any victim" from a violation of the CFAA, including the "cost of responding to" a violation of the CFAA. *Id.* § 1030(e)(11). Courts in this circuit have consistently interpreted this language to reach "the costs of investigating security breaches . . . even if it turns out that no actual data damage or interruption of service resulted from the breach." *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010); *see Saunders Ventures, Inc. v. Salem*, 797 F. App'x 568, 572-73 (2d Cir. 2019) (holding that the record supported a jury verdict for plaintiff on a CFAA claim because plaintiff had introduced evidence of costs incurred on an investigation "to identify evidence of a breach, to assess any damage it may have caused, and to determine whether any remedial measures were needed"); *Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp.*, No. 9-CV-3862, 2010 WL 11591050, at *7 (S.D.N.Y. June 16, 2010) (finding that plaintiff adequately alleged losses from responding to the offense, including "determin[ing] exactly how much confidential material has been downloaded" and "how the information may have been used" by defendants).

Further, while defendants emphasize that plaintiffs were investigating a breach of the Microsoft 365 cloud server, rather than their own computer, *see* Defs.' Br. at 10, courts have

consistently held that the costs incurred in investigating unlawful access to a cloud-based server are cognizable under the CFAA. *See, e.g.*, *Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 926-27 (E.D. Va. 2017) (holding that plaintiffs adequately alleged a violation of the CFAA when defendant unlawfully accessed a cloud storage account); *Prop. Rights Law Grp., P.C. v. Lynch*, No. 13-CV-273, 2014 WL 2452803, at *14 (D. Haw. May 30, 2014) (allowing a claim "based on accessing a 'cloud' platform to proceed as asserting a CFAA violation based on accessing a 'protected computer'"). Plaintiffs have adequately alleged that defendants violated the CFAA and that plaintiffs suffered cognizable losses under the statute. Accordingly, defendants' motion to dismiss the CFAA claim is denied.

CONCLUSION

For the reasons above, defendants' motion to dismiss for failure to state a claim is denied.

SO ORDERED.

/s/ Rachel Kovner
RACHEL P. KOVNER
United States District Judge

Dated: March 11, 2021
Brooklyn, New York